**Before the**
**Federal Communications Commission**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Communications Assistance for | ) | CC Docket No. 97-213 |
| Law Enforcement Act | ) | |



To: The Commission

# REPLY COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER, THE ELECTRONIC FRONTIER FOUNDATION AND THE AMERICAN CIVIL LIBERTIES UNION

David L. Sobel, Esq.
Marc Rotenberg, Esq.
ELECTRONIC PRIVACY INFORMATION CENTER
666 Pennsylvania Avenue, S.E.
Suite 301
Washington, D.C. 20003

Shari Steele, Esq.
ELECTRONIC FRONTIER FOUNDATION
1550 Bryant Street
Suite 725
San Francisco, California 94103

Barry Steinhardt, Esq.
Cassidy Sehgal-Kolbet, Esq.
AMERICAN CIVIL LIBERTIES UNION
125 Broad Street
New York, New York 10004

Kurt A. Wimmer
Alane C. Weixel
Mark E. Porada

COVINGTON & BURLING
1201 Pennsylvania Avenue, N.W.
P.O. Box 7566
Washington, D.C. 20044-7566
202-662-6000

*Attorneys for EPIC, EFF and the ACLU*

Mark J. Emery
Technical Consultant
3032 Jeannie Anna Court
Oak Hill, Virginia 20171

January 27, 1999

## SUMMARY

The Electronic Privacy Information Center, the Electronic Frontier Foundation and the American Civil Liberties Union urge the Commission in its implementation of the Communications Assistance for Law Enforcement Act ("CALEA") to protect the privacy rights of American citizens by finding that the interim standard adopted by the industry and the "punchlist" items proposed by the Department of Justice ("DoJ") and the Federal Bureau of Investigation (FBI") exceed the scope of CALEA and thus should be rejected. The Commission has a fundamental responsibility, mandated by Congress in CALEA, to protect the privacy interest of those using the Nation's telecommunications system.

In adopting CALEA, Congress sought to further three interests: the legitimate surveillance needs of law enforcement; the American public's right to privacy; and the desire to foster new technological inovation. The comments submitted by DoJ/FBI attempt to remove privacy interests from this balance created by Congress. In implementing the capability requirements in CALEA, the Commission may not focus solely on the surveillance needs of law enforcement. Rather, the Commission must take into consideration the other important factors – such as the preservation of privacy interests – enumerated in §§ 103 and 107 of CALEA.

## TABLE OF CONTENTS

Page

**Before the**
**Federal Communications Commission**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Communications Assistance for | ) | CC Docket No. 97-213 |
| Law Enforcement Act | ) | |

To: The Commission

**REPLY COMMENTS OF**
**THE ELECTRONIC PRIVACY INFORMATION CENTER,**
**THE ELECTRONIC FRONTIER FOUNDATION**
**AND THE AMERICAN CIVIL LIBERTIES UNION**

In adopting the Communications Assistance for Law Enforcement Act ("CALEA"), Congress sought to further three interests: the legitimate surveillance needs of law enforcement; the American public's right to privacy; and the desire to foster technological innovation.[1] The comments submitted by the Department of Justice ("DoJ") and the Federal Bureau of Investigation ("FBI") attempt to remove privacy interests from this balance created by Congress. According to DoJ/FBI, in adopting capability requirements, the only interest that the Commission may consider is the surveillance needs of law enforcement.

Although Congress adopted CALEA in response to law enforcement's concerns that new technologies could erode surveillance capabilities, Congress also extended privacy protections to new technologies and technical surveillance standards. Congress gave to the Commission the

[1] H.R. Rep. No. 103-827, pt. 1, at 13 (1994) ("Therefore, the bill seeks to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.").

responsibility to ensure that privacy interests are accorded the highest priority in the implementation of CALEA. The Commission may not disregard this responsibility in favor of law enforcement's surveillance interests. The Electronic Privacy Information Center ("EPIC"), the Electronic Frontier Foundation ("EFF") and the American Civil Liberties Union ("ACLU") urge the Commission to implement the surveillance capability requirements in CALEA in a manner that is consistent with the privacy protections of CALEA, the Constitution and Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III" or the "1968 Wiretap Act").

## I. CONTRARY TO THE ARGUMENTS MADE BY DOJ/FBI, THE COMMISSION IS REQUIRED TO CONSIDER BOTH PRIVACY CONCERNS AND IMPLEMENTATION COSTS WHEN DETERMINING WHETHER CALL-IDENTIFYING INFORMATION IS "REASONABLY AVAILABLE."

The Commission has tentatively concluded that before it can determine "whether a specific technical requirement meets the mandates of Section 103's assistance capability requirements, the Commission must determine whether the information to be provided to [law enforcement] under Section 103(a)(2) is reasonably available to the carrier."[2] It is perfectly appropriate for the Commission first to consider whether information sought by law enforcement is reasonably available, before determining whether production of such information falls within the capability requirements of CALEA. CALEA requires that *both* considerations be satisfied before a carrier can be required to provide specific information to law enforcement. The mere fact that information sought by law enforcement is reasonably available cannot lead to the automatic conclusion that such information must be produced to law enforcement officers.

[2] Communications Assistance to Law Enforcement Act, CC Docket No. 97-231, *Further Notice of Proposed Rulemaking*, FCC 98-282, ¶ 25 (Nov. 5, 1998) (the "*Further Notice*").

Conversely, "call identifying information"[3] cannot be provided to law enforcement if it is not reasonably available. Carriers only are obliged to provide access to "call-identifying information" that is "reasonably available."[4]

DoJ/FBI claim that reasonable availability is a "technical concept" completely unrelated to considerations of cost or any of the other important factors, such as the preservation of privacy interests, enumerated in §§ 103 and 107 of the statute.[5] According to the DoJ/FBI Comments, the Commission need not burden itself with considering the costs of implementing the industry standard or the DoJ/FBI punchlist items during a rulemaking proceeding under § 107. DoJ/FBI argue that costs and other concerns only are relevant *after* the Commission has promulgated CALEA standards, when a carrier seeks a waiver of compliance with those standards under § 109 because such standards are not "reasonably achievable" by the carrier. Quite simply, the DoJ/FBI's reading of CALEA is untenable and reads privacy out of the statute.

Section 103 of CALEA, which defines a carrier's obligations under the statute, requires carriers to provide law enforcement access only to call-identifying information that is "reasonably available."[6] Moreover, carriers must provide call-identifying information in a manner that protects the "privacy and security of communications and call-identifying

---

[3] "Call-identifying information" is defined narrowly as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." CALEA § 102(2), 47 U.S.C. § 1001(2).

[4] CALEA § 103(a)(2), 47 U.S.C. § 1002(a)(2).

[5] DoJ/FBI Comments Regarding Further Notice of Proposed Rulemaking at 2 ("DoJ/FBI Comments").

[6] CALEA § 103(a)(2), 47 U.S.C. § 1002(a)(2).

information not authorized to be intercepted."[7] In a rulemaking proceeding under § 107, the Commission is empowered "to establish, by rule, technical requirements or standards that—(1) meet the assistance capability requirements of section 103 by cost-effective methods; [and] (2) protect the privacy and security of communications not authorized to be intercepted."[8] Thus, the Commission is statutorily bound to consider both cost and privacy concerns when issuing regulations pursuant to § 107 to implement carriers' obligations under § 103.

The DoJ/FBI Comments engage in semantics to argue that § 107 does not address *whether* a carrier will be required to comply with CALEA, only *how* it will comply.[9] At first glance, DoJ/FBI are quite correct, in that § 107 addresses the scope of permissible regulations the Commission can adopt to implement the requirements of § 103. Upon closer examination, however, it is clear that DoJ/FBI's assertion is little more than a red herring that is more distracting than useful.

One cannot argue with DoJ/FBI's position that the Commission is charged under § 107 with the authority to define how carriers can comply with the requirements imposed in § 103. But that argument merely begs the question of what requirements, exactly, are imposed in § 103. As stated above, § 103 makes it clear that CALEA does not require that call-identifying information be provided to law enforcement if such information is not "reasonably available." Likewise, § 103 imposes a restriction on law enforcement's access to such information if it would interfere with protected privacy interests. In the express delegation of authority contained

[7] CALEA § 103(a)(4)(A), 47 U.S.C. § 1002(a)(4)(A).

[8] CALEA § 107(b), 47 U.S.C. § 1006(b).

[9] DoJ/FBI Comments at 11.

in § 107, the Commission is directed to promulgate rules that are both cost-effective and protect the privacy and security of confidential communications.

DoJ/FBI would have the Commission believe that, if it issues regulations denying law enforcement access to any form of call-identifying information, it is violating the access requirements of CALEA. Such a selective reading of CALEA is illogical and inconsistent with the express language of the statute. While the Commission is, indeed, charged in § 107 with the duty to define *how* carriers must comply with the requirements of § 103, the Commission may not use that authority to define the manner of compliance in a way that requires carriers to provide law enforcement access to information that *exceeds* the scope of the statute.

DoJ/FBI argue that, because cost concerns can be considered by the Commission in a § 109 proceeding after the Commission has adopted industry standards, the Commission is therefore precluded from considering such matters at this point. Section 109 provides that a carrier may petition the Commission for a determination of "whether compliance with the assistance capability requirements of section 103 is reasonably achievable with respect to any equipment, facility, or service installed or deployed after January 1, 1995."[10] In a § 109 proceeding, the Commission is directed to determine whether compliance with the standard "would impose significant difficulty or expense on the carrier or on the users of the carrier's system," while considering, among other things: (1) "the need to protect the privacy and security of communications not authorized to be intercepted"; and (2) "the need to achieve the capability assistance requirements of section 103 by cost-effective methods."[11]

[10] CALEA § 109(b)(1), 47 U.S.C. § 1008(b)(1).

[11] CALEA §§ 109(b)(1)(C), (D), 47 U.S.C. §§ 1008(b)(1)(C), (D).

The DoJ/FBI argument, essentially, is that the Commission simply should adopt regulations requiring law enforcement access to call-identifying information without consideration of any cost issues, regardless of the Commission's obligation to do so under §§ 103 and 107, because carriers would be able to raise any cost concerns later on after the regulations were adopted. Although the DoJ/FBI Comments do not specifically state that the Commission should take the same approach with any privacy concerns raised at this juncture, the same reasoning would apply. Because carriers are capable of seeking a waiver of compliance with adopted industry standards under § 109, which directs the Commission to consider privacy infringement when deciding whether compliance with the standards would impose difficulty or expense on the carrier, the objections by privacy groups simply could be brushed aside.

Although it is likely that carriers would file § 109 petitions if the Commission decides to adopt standards without regard to cost concerns, it is unlikely that any carrier would file a § 109 petition solely on the grounds that the adopted industry standard is not "reasonably achievable" because of interference with the privacy or security of protected communications. Thus, the DoJ/FBI's argument that cost-effectiveness and, by implication, privacy interests, may be shunted aside until after the Commission has actually adopted rules, is both unlawful and impractical. The Commission must not adopt the DoJ/FBI's reasoning as a means of postponing resolution of difficult privacy and cost concerns.

Furthermore, the DoJ/FBI's reading of "reasonably available" makes the term meaningless.[12] If the Commission does not take into account costs, privacy concerns or any of

[12] The Commission must consider CALEA as a whole and may not interpret the statute in a manner that makes some of its provisions meaningless, simply because the same issues can be raised under another statutory provision. *See Beecham v. United States*, 511 U.S. 368, 372 (1994) (stating that in interpreting a statute, one must consider "the plain meaning of the whole (continued...)

the other enumerated factors in §§ 103 and 107, then it is hard to imagine how any information to which law enforcement seeks access would not be deemed "reasonably available." While that result undoubtedly would suit law enforcement well, it would be a blatant violation of the express terms of CALEA.[13]

The Commission has been assigned a unique and vital role in the implementation of CALEA. While DoJ/FBI would have the Commission believe its purpose is limited to rubber-stamping any requests for additional law enforcement access to confidential communications in the quest to eradicate crime, Congress chose to place implementation of the statutory requirements in an independent agency for a special reason. As the structure and legislative history of CALEA make clear, Congress intended for the Commission to review the sufficiency of industry technical standards to ensure that important privacy interests of Americans would be protected.[14] The Commission must reject the DoJ/FBI's interpretation of "reasonably available"

---

statute, not of isolated sentences); *see also King v. St. Vincent's Hosp.*, 502 U.S. 215, 221 (1991); *Massachusetts v. Morash*, 490 U.S. 107, 115 (1989); *Shell Oil Co. v. Iowa Dept. of Revenue*, 488 U.S. 19, 26 (1988).

[13] Although the ACLU, EPIC and EFF have no independent analyses of the costs involved in implementing the industry standard and the DoJ/FBI's punch list items, submissions by carriers and industry representatives project costs soaring into the billions of dollars, well above the $500 million allocated by Congress to reimburse carriers for their costs. *See* CALEA §§ 109(b)(2), 110, 47 U.S.C. §§ 1008(b)(2), 1009; United States Telephone Association Comments at 8 (implementation of industry standard and punch list items by members would cost over $2.2 billion); Ameritech Comments at 4 (implementation would cost $69 million); GTE Comments at 7 (implementation of industry standard alone would cost $400 million); Bell South Comments at 5-6 (implementation of industry standard would cost $128 million and an additional $175 million for punch list items). It is hard to understand how such costs could be "reasonable" in light of the fact that they exceed by several times the amount Congress considered appropriate for industry redevelopment costs. As such, the industry standard and the punch list items should be rejected because the information they seek to require is not "reasonably available."

[14] *See* H.R. Rep. No. 103-827 at 17-18 (stating that CALEA includes a provision, previously supported by the FBI, that "add[s] protections to the exercise of the government's current (continued...)

and fully consider the implications on protected privacy interests, as well as costs, when adopting industry access requirements.

## II. ISSUES RAISED BY THE PROPOSED INTERIM STANDARD

### A. The Commission's Tentative Conclusion Regarding Packet-Mode Communications Is Correct.

The Commission's cautious approach in adopting CALEA capability requirements for packet-mode systems is the correct approach. The use of packet-mode systems to transmit voice and data communications is expected to grow rapidly in the future and indeed may become the prevailing method for transmitting communications. It is therefore critical that the CALEA capability requirements established by the Commission adequately protect the privacy of communications carried on packet-mode systems. As the Commission noted in its *Further Notice*, "packet-mode issues are complex."[15] We commend the Commission's willingness to use additional time or proceedings to resolve correctly these complex issues and to preserve the privacy of our nation's communications.

The J-Standard requires carriers transmitting communications using packet-mode systems to deliver the entire packet data stream associated with a given communication -- including the call content -- to law enforcement, even if law enforcement is authorized to receive only call-identifying information. Although § 103(a)(4)(A) of CALEA *requires* carriers to provide intercepted communications to law enforcement "in a manner that protects . . . the privacy and security of communications and call-identifying information not authorized to be intercepted,"

---

surveillance authority," by requiring the Commission to consider whether the industry standards "protect the privacy of communications not authorized to be intercepted").

[15] *Further Notice*, ¶ 66.

DoJ/FBI nonetheless maintain that the J-Standard's treatment of packet-mode communications "does not conflict with anything in CALEA."[16]

Not surprisingly, DoJ/FBI fail to offer a reasoned explanation for this conclusion. DoJ/FBI contend that a carrier's reliance on law enforcement to minimize communications not authorized to be intercepted satisfies that carrier's duty to protect the "privacy and security of communications."[17] Were Congress satisfied that law enforcement would adequately minimize communications, there would have been no need to impose a separate requirement on carriers.

As DoJ/FBI correctly state, "the statutory requirements of § 103 do apply to packet mode communications[.]" That means *all* of § 103 applies, including the requirement that carriers protect the security and privacy of communications. Permitting carriers to provide law enforcement with all of the contents of a subscriber's telephone conversations when law enforcement is authorized only to receive call identifying information is patently inconsistent with the privacy requirements of § 103.[18] DoJ/FBI may not selectively read out of the statute those provisions which limit law enforcement's ability to conduct electronic surveillance.

According to the industry, call-identifying information cannot, at this time, be separated from call content in packet-mode systems. In other words, call-identifying information for packet-mode systems is not "reasonably available to the carrier" as required under § 103(a)(2). Further evaluation of packet-mode systems may identify a means for carriers to satisfy fully the requirements of § 103. However, until carriers are able to protect the privacy of communications

---

[16] DoJ/FBI Comments at 79.

[17] DoJ/FBI Comments at 80.

[18] As explained in the initial comments filed by EPIC/EFF/ACLU, allowing law enforcement to obtain call content with only a pen register would also violate the "particularity" requirements of the Fourth Amendment and Title III of the 1968 Wiretap Act. *See* EPIC/EFF/ACLU Comments at 11-13.

carried over packet-mode systems, the Commission should refrain from adopting capability requirements for such communications.

### B. The Location Tracking Provisions Contained In The Industry Standard And As Tentatively Endorsed By The Commission Are Not Permitted By CALEA.

DoJ/FBI agree with the Commission's tentative conclusion that the industry standard is designed to require provision of location tracking information at the beginning and end of a wireless telephone call. DoJ/FBI argue that location tracking information is call-identifying information for purposes of CALEA because it identifies the "origin" or "destination" of a call, and therefore must be provided in all situations, except where law enforcement is proceeding solely with pen register or trap and trace authority.[19] The government's reading of the statute is both inaccurate and far broader than Congress intended.

CALEA contains no provisions expressly including location tracking data within the definition of call-identifying information. On the contrary, it is clear from the legislative history that Congress never intended for carriers to have to provide location tracking information to law enforcement. The House Report provides that carriers are obliged to "isolate expeditiously information identifying the originating and destination number of targeted communications, but not the physical location of targets."[20] In defining call-identifying information, the House Report concludes that such information consists of "the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted for the purpose of routing calls through the telecommunications carriers' network."[21] It is obvious from the legislative

---

[19] DoJ/FBI Comments at 75.

[20] H.R. Rep. No. 103-827 at 17.

[21] *Id.* at 21.

history that Congress never contemplated requiring carriers to provide information concerning a subject's physical location as part of their CALEA obligations.

The industry standard itself, upon which the Commission tentatively relied in the *Further Notice*, is internally inconsistent. On the one hand, the industry standard proposes to require carriers to provide location tracking data at the beginning and at the end of calls, as part of carriers' duties to provide information regarding the "origin" and "destination" of particular communications. But the definitions of those terms within the industry standard have nothing to do with physical location.

The industry standard includes the following definitions:

> **destination** is the number of the party to which a call is being made (e.g., called party); **direction** is the number to which a call is re-directed or the number from which it came, either incoming or outgoing (e.g., redirected-to party or redirected-from party); **origin** is the number of the party initiating a call (e.g., calling party); and **termination** is the number of the party ultimately receiving a call (e.g., answering party).[22]

None of the four terms, which form the boundaries of what can be considered call-identifying information under CALEA,[23] mention physical location. It is illogical for the industry to define "origin" and "destination" as excluding physical location in one part of the standard, and then agree in another section of the standard that carriers must provide location tracking at the beginning and at the end of calls because such information involves the "origin" and "destination" of those calls. It should be clear from the inconsistencies that the industry standard amounts to nothing more than a compromise between the telecommunications industry and law enforcement. While the industry's attempts to build a consensus with law enforcement

---

[22] J-Standard at 5.

[23] *See* CALEA § 102(2), 47 U.S.C. § 1001(2).

may be laudable, the industry has no right to expand the scope of call-identifying information as defined in CALEA simply to please DoJ/FBI. To the extent that the Commission relies on the industry standard at all, it should look to the standard's definitions of "origin" and "destination" and see that they simply do not support the industry's decision to provide location tracking information to law enforcement.

Although Congress did not require carriers to implement location tracking technology or provide such information to law enforcement under CALEA, it recognized that some carriers might voluntarily decide to use services or facilities with tracking features for business purposes or to fulfill other, unrelated obligations. Congress did not wish to inhibit carriers from adopting new technology, but yet, to the extent carriers developed such technology, Congress sought to restrict law enforcement's access to tracking data compiled thereby. To achieve that end, Congress included a provision in CALEA providing that, "with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices ... such call-identifying information shall *not* include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)."[24]

As other commenters have argued, CALEA was intended to create two different obligations: the duty to implement certain technical changes to permit law enforcement to gain access to particular information; and the obligation to provide additional information to law enforcement if the carrier's system voluntarily produces that data.[25] As stated above, the plain language of the statute and its legislative history show that Congress did not intend to mandate

[24] CALEA § 103(a)(2)(B), 47 U.S.C. § 1002(a)(2)(B) (emphasis added).

[25] *See* Center for Democracy & Technology Comments at 10 ("CDT Comments").

provision of location tracking information to law enforcement. Section 103(a)(2)(B) was meant to address situations where carriers' systems happen to produce that information for independent, unrelated reasons. By the express terms of the statute, which restricted pen register and trap and trace access to "the dialing and signaling information utilized in call processing,"[26] Congress precluded law enforcement from gaining access to that information with only pen register or trap and trace authority.[27]

DoJ/FBI also argue that location tracking information will be produced by carriers anyhow, as a result of their enhanced 911 ("E911") obligations.[28] As addressed in our earlier comments, the fact that E911 obligations may require carriers to implement tracking technology that permits emergency personnel to trace the location of a caller who dials 911 does not mean that tracking information automatically must be provided to law enforcement under CALEA, simply because the technology already may exist. Law enforcement has no basis for acquiring location tracking information simply because it may be "reasonably available" pursuant to carriers' E911 responsibilities. CALEA does not authorize law enforcement to gain access to communications information based on whether carriers already produce that information for unrelated purposes. Rather, the statute restricts law enforcement access to call-identifying

---

[26] CALEA § 207(c), 18 U.S.C. § 3121(c).

[27] DoJ/FBI tacitly have acknowledged that § 103(a)(2)(B) was designed to address situations where carriers voluntarily produce location tracking data that is beyond the scope of CALEA. DoJ/FBI have conceded that, in such situations, carriers need not provide expanded location tracking data absent a court order. *See* DoJ/FBI Comments at 75 n.9. If DoJ/FBI agree that § 103(a)(2)(B) was intended to address access to location tracking information that carriers are not required to produce, the Commission's tentative conclusion that the statute was intended to *require* carriers to produce tracking information at the beginning and end of calls is incorrect.

[28] Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling, Report & Order and *Further Notice* of Proposed Rulemaking, 11 FCC Rcd. 18676 (1996), *modified in part on reconsideration,* Memorandum Opinion and Order, 12 FCC Rcd. 22665 (1997).

information, as defined therein.[29] Location tracking information does not fall within that definition.

In addition, it is by no means clear that the E911 location tracking capability would permit most carriers to provide the kind of location tracking information sought by law enforcement under CALEA at the beginning and end of each call. As industry groups have pointed out, "for many manufacturers the development of E911 location tracking and CALEA location information is distinctly separate."[30] Industry commenters have acknowledged that "Congress wanted to avoid turning wireless handsets into tracking devices." [31] Nevertheless, they support the industry standard location tracking provisions because they strike a balance between competing law enforcement and privacy interests. What the Commission has to recognize, however, is that the ultimate purpose of CALEA was not to encourage the telecommunications industry and law enforcement to compromise. The purpose was to ensure that law enforcement had continued access to the kinds of information it previously obtained in a wired, analog environment, while protecting important privacy concerns affected by the development of new technologies. The Commission must not lose sight of that purpose in a rush to congratulate the industry and law enforcement for working together to strip CALEA of the protections included by Congress.

---

[29] CALEA § 103(a)(2), 47 U.S.C. § 1002(a)(2).

[30] Telecommunications Industry Assoc. Comments at 49 n.117 ("TIA Comments").

[31] *Id.* at 48.

## III. ISSUES RAISED BY THE DOJ/FBI "PUNCHLIST"

### A. Law Enforcement Agencies Have No Right Of Access To Post-Cut-Through Digits From An Initial Carrier Under CALEA.

DoJ/FBI seek to acquire post-cut-through digits from initial carriers on the grounds that the digits are call-identifying information, because they identify the "destination" of a communication.[32] According to the government, it does not matter whether the digits are actually treated as call-identifying information for an initial carrier, as long as they are so considered by any later carrier. In other words, DoJ/FBI argue that CALEA includes no requirement that post-cut-through digits be used for call routing purposes by the carrier from which law enforcement seeks call-identifying information. According to DoJ/FBI, once the information is classified as call-identifying information by any carrier involved in a communication, then it is call-identifying information for all prior carriers (even though the information was transmitted on the initial carriers' call content channels).

The government has given CALEA a twisted and unnatural reading. The fact that a long-distance carrier may consider certain digits for call routing purposes, which makes them call identifying information for the long-distance carrier, has no bearing on whether an initial carrier uses those digits for call routing. To the initial carrier, the post-cut-through digits do not identify the "destination" of a call, because they are considered call content once the call is connected to the long-distance carrier. The Commission must give CALEA a natural reading and give the statute's terms their ordinary meaning.[33] It is implausible that Congress intended for law

---

[32] DoJ/FBI Comments at 66.

[33] *See, e.g.*, *Patterson v. Shumate*, 504 U.S. 753, 760 (1992) (stating that a party seeking to defeat the plain meaning of statutory terms bears an "exceptionally heavy burden"); *Perrin v. United States*, 444 U.S. 37, 42 (1979) (stating that statutory words should be given their ordinary meaning).

enforcement to be able to obtain post-cut-through digits from initial carriers as call-identifying information, when those digits have nothing to do with a call's "destination" or "direction" from the initial carrier's perspective.[34] Because sensitive content typically is mixed in an initial carrier's call-content channel with other digits ultimately used for call-routing by a subsequent carrier, the total stream of post-cut-through digits cannot be classified as call-identifying information. To safeguard the privacy of such sensitive information, as the Commission statutorily is bound to do, the DoJ/FBI's request for access to post-cut-through digits must be denied.

DoJ/FBI argue that it would be unduly burdensome for law enforcement to rely on pen register orders served on long-distance carriers to gain access to post-cut-through digits. The government argues that that procedure would require a long distance carrier to monitor every incoming call and cross-check the incoming telephone number with every outstanding pen register order.[35] The DoJ/FBI Comments paint a picture more reminiscent of the 1940s than today, one in which a host of switchboard operators manually connect each incoming call to its destination without the aid of any computerized or automated equipment. In reality, it seems likely that every incoming telephone call initially is processed through an automated system which has the capability of recognizing the incoming telephone number and comparing that number to any pen registers entered into the system. Undoubtedly, law enforcement currently serves pen register orders on long-distance carriers and succeeds in recording incoming or outgoing telephone numbers without undue burden. Because CALEA was not intended to

---

[34] According to TIA, the DoJ/FBI previously conceded that post-cut-through digits are call content for initial carriers, and that law enforcement would obtain Title III warrants to gain access to that information from initial carriers. *See* TIA Comments at 40 n.99.

[35] DoJ/FBI Comments at 69.

enhance law enforcement's ability to engage in electronic surveillance, the DoJ/FBI argument should be rejected.[36]

DoJ/FBI also argue that the Commission should reject the industry standard provision addressing post-cut-through digits, which only requires carriers to provide access to information present at the originating carrier's Intercept Access Points ("IAPs"), because "failure to do so would effectively nullify the Commission's tentative conclusion that post-cut-through dialing is call-identifying information."[37] But the Commission's tentative conclusion is exactly that—it is tentative. The Commission is not bound by its suggestion in the *Further Notice* and it need not adhere to its tentative conclusion concerning post-cut-through digits simply for the sake of consistency. As a general matter, "the tentative conclusions of the NPRM are of no decisional significance."[38]

CALEA specifically provides that carriers used for the "switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers" are not required to comply with CALEA's access requirements, beyond permitting law enforcement to "identify the new service provider handling the communication."[39] Congress contemplated that carriers used by a subscriber merely to connect to a long-distance service are not responsible for providing law enforcement with anything other than the identity of the subsequent carrier. Beyond that, an initial carrier has no obligation to excise post-cut-through digits used for call routing from other call content.

---

[36] H.R. Rep. at 103-827 at 13 ("Therefore, the bill seeks to ... preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts").

[37] DoJ/FBI Comments at 69.

[38] In re Southwestern Bell Telephone Company, CC Docket No. 97-158, *Order*, 12 FCC Rcd. 19311, ¶ 55 (Nov. 14, 1997).

[39] CALEA § 103(b)(2)(B), 47 U.S.C. § 1002(b)(2)(B).

According to TIA, no originating carrier currently captures post-cut-through digits, because there are no business reasons to do so.[40] DoJ/FBI concede that there currently is no technology that would permit initial carriers to separate certain post-cut-through digits from other information contained on a call-content channel.[41] The industry has estimated that the development of such technology would be prohibitively expensive, to the extent it is possible in the near future at all.[42] Because carriers would not have any business purposes for developing and implementing technology permitting them to separate post-cut-through digits, their operating expenses would rise with no counter-balancing benefit. Undoubtedly this would impact on costs for consumers, violating the twin statutory requirements of "meet[ing] the assistance capability requirements of section 103 by cost-effective methods," and "minimiz[ing] the costs of such compliance on residential ratepayers."[43]

Post-cut-through digits are not utilized for call-routing purposes by initial carriers and, as such, are not call-identifying information because they do not signal a call's "destination" or "direction" for the initial carrier. Every commenter seems to agree that there is no feasible way to separate post-cut-through digits used for call-routing from other sensitive information transmitted on an initial carrier's call content channel. The development of technology capable of separating post-cut-through digits would require extensive engineering modifications to switches used in wireline systems and software used in wireless systems. Even if the information were considered call-identifying information for an initial carrier, that information is not "reasonably available" and need not be provided to law enforcement under CALEA.

---

[40] TIA Comments at 24.

[41] DoJ/FBI Comments at 67.

[42] TIA Comments at 41-42.

### B. DoJ/FBI Have Failed To Justify Their Expansive Definition Of The Term "Facilities" As It Applies To Surveillance Of Conference Calls.

As set forth in the initial comments filed by EPIC, EFF and the ACLU, the Commission's tentative conclusion to require that law enforcement have the ability to monitor conversations connected via conference call even after the subject, or someone using the subjects facilities, drops off significantly expands the "facilities" doctrine of Title III of the Omnibus Crime Control and Safe Street Act of 1968 ("Title III" or the "1968 Wiretap Act").[44] "Facilities" have traditionally been considered for Title III purposes as the subscriber's terminal equipment. The comments filed by DoJ/FBI confirm that they seek to expand the "facilities" doctrine to include all network facilities that are used in any way to provide service to the subject.

Section 103(a)(1) requires carriers to provide law enforcement with access to all communications transmitted by that carrier "to or from equipment, facilities, or services of a subscriber . . . ." In interpreting the phrase "equipment, facilities, and services," DoJ/FBI contend that "[a] subscriber's 'equipment' and 'facilities' encompass all of the elements of the carrier's network that support and are identifiable with the services that the carrier provides to the subscriber."[45] In other words, any part of a carrier's network that in any way is used to provide a service to the subscriber would be considered the subscriber's "facilities" under § 103(a)(1) of CALEA, and carriers would have to make available to law enforcement any conversations carried over those network facilities. Under this expansive definition of "facilities," any conference call initiated by the target's terminal equipment would be subject to an ongoing

---

[43] CALEA §§ 107(b)(1), (3), 47 U.S.C. §§ 1006(b)(1), (3).

[44] EPIC/EFF/ACLU Comments at 20-22.

[45] DoJ/FBI Comments at 38.

intercept – even after the target's phone is disconnected – so long as the call continues to be carried somewhere on the carrier's network.

DoJ/FBI make no attempt to harmonize this wildly expansive definition of "facilities" with the instruction from Congress "against overbroad interpretation of [CALEA's] requirements" and that industry, law enforcement and the FCC should "narrowly interpret the [CALEA] requirements."[46] On the contrary, DoJ/FBI have acknowledged that this would be an expansion of law enforcement's current capabilities, even though the FBI Director told Congress, at the time it was considering the CALEA legislation, that CALEA "was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information that it had in the past.[47] Given this clear legislative history that CALEA is not to be used to expand law enforcement's surveillance capabilities, DoJ/FBI's definition of "facilities" cannot be sustained. Rather, the definition of "facilities" must continue to be limited to a subscriber's terminal equipment. And, once the target's terminal equipment is no longer in use, surveillance of the call ceases.[48]

### C. DoJ/FBI Have Failed To Justify Their Expansive Definition Of Call-Identifying Information.

DoJ/FBI continue to sweep within the definition of "call-identifying information" other types of signaling information that fall outside the scope of CALEA, and also seek to include access to information services as call-identifying information. "Call-identifying information" is defined as "dialing or signaling information that identifies the origin, direction, destination, or

---

[46] H.R. Rep. No. 103-827.

[47] *Id.*

[48] As explained in the initial comments filed by EPIC, EFF, and the ACLU, expanded access to conference call content would also violate the privacy protections of the Fourth Amendment. *See* EPIC/EFF/ACLU Comments at 24.

termination" of a communication.[49] Call-identifying information has always represented simply the telephone number indicating the origination or destination of a call. The legislative history of CALEA confirms that call-identifying information is limited to "electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted for the purpose of routing call through the telecommunications network."[50] To emphasize that call-identifying information is limited to pulses and tones that identify incoming or outgoing phone numbers, Congress further stated that "[o]ther dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information."[51]

Neither the Commission nor DoJ/FBI try to reconcile their interpretation of "call-identifying information" with this legislative history. Rather, both adopt a strained definition of "origin, direction, destination or termination" in order to fit within the definition of call-identifying information party hold/join/drop messages. This is most obvious with regard to party hold messages. According to the Commission, for purposes of CALEA, placing a party on hold amounts to a "temporary termination" of the call.[52] However, the call has not been disconnected nor has it ended. In no other context would placing a party on hold be considered a "termination" of the call. It is being done in this instance in an effort to force-fit party hold/join/drop messages within the definition of call-identifying information. However, since Congress directed the Commission to interpret CALEA narrowly, expanding the definition of call-identifying information to include party join/drop/hold messages is impermissible.

---

[49] CALEA, § 102(2), 47 U.S.C. § 1001(2).

[50] H.R. Rep. No. 103-827 at 21.

[51] *Id.*

In the course of reiterating their contention that a subject's use of feature keys or the flash hook also falls within the definition of call-identifying information, DoJ/FBI also appear to argue that law enforcement may obtain the contents of a voice mailbox under § 103(a). As the Commission correctly noted, the contents of a subject's voice mailbox fall outside the scope of CALEA.[53] The capability requirements in § 103(a) do not apply to "information services."[54] "Information services" include "a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities."[55] The legislative history clarifies that although the "redirection of [a] voice mail message to the 'box' . . . [is] covered" under CALEA, the "storage of a message in a voice mail . . . 'box' is not covered[.]" To the extent that a carrier provides a service that allows a subscriber to retrieve a voice mail message, that carrier is operating as an information service provider and that service is not subject to the capability requirements in § 103(a). DoJ/FBI may not obtain access to a subscriber's voice mailbox by classifying a subscriber's retrieval of a voice mail message as a "communication" or as "call-identifying information" under § 103(a).

---

[52] *Further Notice*, ¶ 85.

[53] *Further Notice*, ¶ 93.

[54] CALEA, § 103(b)(2), 47 U.S.C. § 1002(b)(2).

[55] CALEA, § 102(6)(B), 47 U.S.C. § 1001(6)(B).

## IV. CONCLUSION

For the foregoing reasons and the reasons set forth in the initial comments filed by EPIC/EFF/ACLU, we urge the Commission to reject the industry standard and the DoJ/FBI punchlist proposals and to exercise its duty under CALEA to protect the privacy rights of our nation's telephone subscribers.

Respectfully submitted,


Kurt A. Wimmer
Alane C. Weixel
Mark E. Porada

COVINGTON & BURLING
1201 Pennsylvania Avenue, N.W.
P.O. Box 7566
Washington, D.C. 20044-7566
202-662-6000

*Attorneys for EPIC, EFF and the ACLU*

David L. Sobel, Esq.
Marc Rotenberg, Esq.
ELECTRONIC PRIVACY INFORMATION CENTER
666 Pennsylvania Avenue, S.E.
Suite 301
Washington, D.C. 20003

Shari Steele, Esq.
ELECTRONIC FRONTIER FOUNDATION
1550 Bryant Street
Suite 725
San Francisco, California 94103

Barry Steinhardt, Esq.
Cassidy Sehgal-Kolbet, Esq.
AMERICAN CIVIL LIBERTIES UNION
125 Broad Street
New York, New York 10004

Mark J. Emery
Technical Consultant
3032 Jeannie Anna Court
Oak Hill, Virginia 20171


January 27, 1999